Sengathir and Manoharan *EURASIP Journal on Wireless Communications and Networking* (2015) 2015:158
DOI 10.1186/s13638-015-0384-4

EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

A futuristic trust coefficient-based semi-Markov prediction model for mitigating selfish nodes in MANETs

Janakiraman Sengathir* and Rajendiran Manoharan

Abstract

In mobile ad hoc networks (MANETs), network survivability is considered as a potential factor required for maintaining maximum degree of connectivity among the mobile nodes even during failures and attacks. But, the selfish mobile nodes pose devastating influence towards network survivability. Hence, a prediction model that assesses network survivability through stochastic properties derived from nodes' behaviour becomes essential. This paper proposes a futuristic trust coefficient-based semi-Markov prediction model (FTCSPM) that investigates and quantifies the impact of selfish behaviour towards the survivability of the network. This FTCSPM approach incorporates a non birth-death process for manipulating futuristic trust coefficient since it does not consider the transition of a mobile node from the failed state to a selfish state into account. This semi-Markov prediction model also aids in framing a lower and upper bound for network survivability. Extensive simulations were carried out through ns-2 and the results indicates that FTCSPM show better performance than the existing benchmark mitigation mechanisms like correlated node behaviour model (CNBM), probabilistic behavior model (PBM) and epidemic correlated node behavioural model (ECNBM) proposed for selfish nodes. Further, FTCSPM isolates the selfish nodes rapidly at the rate of 33 % than the considered benchmark systems. Furthermore, the validation of this prediction model performed through Weibull distribution has a high degree of correlation with the simulation results and thus assures the reliability and correctness of the proposed approach. In addition, this approach computes the mean transition time incurred by a mobile node to transit from cooperative to selfish mode as 6.49 s and also identifies the minimum and maximum selfish behaviour detection time as 140 and 180 s, respectively.

Keywords: Futuristic trust coefficient; Selfish nodes; Network survivability; Semi-Markov prediction model; Non birth-death process

1 Introduction

In mobile ad hoc networks (MANETs), network survivability is considered as an important entity for reliable data communication. But the dynamic change in mobile nodes' behaviour pose a great challenge towards the survivability of the network since they do not possess a centralised infrastructure for communication [1]. Moreover, the transition of mobile nodes' behavioural state from cooperation to selfish drastically affects the connectivity of the network [2]. Further, mobile ad hoc networks are highly prone to random failures and attacks due to their unique characteristics like limited energy availability, dynamic network infrastructure and error-prone communication link [3]. Thus, in practical, a mobile ad hoc network is said to be highly survivable when it establishes and maintains a collaborative environment among the mobile nodes [4].

From the recent past, researchers have analysed the survivability of the network in terms of network connectivity [5–7]. This network connectivity highly depends on the degree of cooperation attributed by the mobile nodes present in the routing path established between the source and the destination [8]. This degree of cooperation is drastically affected by means of selfish behaviour since selfish nodes deny forwarding either data or control packets of their neighbouring nodes for conserving its energy. In addition, the selfish behaviour of a

* Correspondence: j.sengathir@gmail.com
Department of Computer Science and Engineering, Pondicherry Engineering College, East Coast Road, Pillaichavady, Puducherry 605013, India

mobile node prevents an individual node from participating in routing activity and affects the cooperation level rendered by the mobile nodes present in the routing path.

In the literature, various mitigation mechanisms proposed for selfish nodes either concentrates on the past history of mobile nodes or estimates conditional probabilistic factor based on both the past and present behaviour of the mobile node into account [9, 10]. However, these approaches lack to detect selfish nodes by forecasting the probability of transition between the behavioural states of the mobile nodes based on its present characteristics.

In this paper, we contribute a futuristic trust coefficient-based semi-Markov prediction model to forecast the likelihood ratio of a mobile node to turn into selfish based on stochastic properties derived from its present behaviour. This semi-Markov prediction model incorporates a non birth-death Markov process, which is a special kind of Markov chain that does not emphasize on the restriction of nearest neighbour only transitions. Further, we assume that a failed mobile node cannot be converted into a selfish node. Hence, in this prediction model, a Markov chain is utilized for modeling the node behaviour transitions. Furthermore, this model considers three possible types of node behaviours viz., cooperative, selfish and failed. In addition, ad hoc on-demand distance vector (AODV) protocol has been modified with an additional metric called as expected level cooperation coefficient pertaining to the next hop neighbour in order to establish reliable route for data dissemination.

The major contributions of this semi-Markov model are as follows:

1) This paper investigates on semi-Markov prediction model to forecast the mobile nodes' behaviour manipulated through the present state characteristics represented by means of futuristic trust coefficient.
2) The survivability of the mobile ad hoc network is estimated probabilistically, and the upper and lower thresholds for network connectivity are derived in this paper.
3) This paper provides a semi-Markov model that is validated using Weibull distribution since it is the predominant distribution used for evaluating lifetime in reliability-based engineering.

The remaining part of the paper is organized as follows. Section 2 presents in-depth analysis about the existing selfish behaviour prediction models in the literature. Section 3 depicts the futuristic trust coefficient-based semi-Markov prediction model that aids in forecasting the change in mobile nodes' behaviour towards selfishness. Section 4 briefly describes the influence of selfish nodes towards network survivability and model validation using Weibull distribution. Section 5 presents the details of the simulation environment and the comparative analysis performed with the benchmark systems and the proposed FTCSPM. Section 6 concludes the paper with future plan of work.

2 Related work

In the literature, considerable number of models which extensively analyses the survivability of mobile ad hoc networks in the presence of various types of malicious nodes is discussed. Xing and Wang [11] presented an analytical approach to evaluate network survivability in the presence of misbehaving nodes and failure nodes. In their work, authors investigated a novel mechanism based on semi-Markov process that categorizes mobile nodes' behaviour into four types viz., i) cooperative node, ii) failure node, iii) selfish node and iv) malicious node. Authors also incorporated a special type of counter known as the Nuglet counter to estimate the probability of node misbehaviour at any instant of time. This approach also aids in deriving the closed form approximation of network survivability based on network characteristic functionalities and node behaviour distribution.

Further, Cardenas et al. [12] recommended a sequential probability ratio test (SPRT) detection scheme which incorporates a quantitative approach called DOMINO for mitigating selfish behaviour in an ad hoc network. This work adopts a dual step process for detecting selfish behaviour of a mobile node. In the first step, the transition probability of mobile nodes which are currently under direct communication was estimated. In the second step, Markov chain was derived for each mobile node with transition probability p and 1-p. Finally, the identification of misbehaving mobile nodes was carried out by monitoring the state changes through Markov chain. Vallam et al. [13] incorporated a discrete time Markov chain (DTMC) with steady-state probabilities for analysing non saturated node. This mechanism addresses the problem of back-off manipulation that arises due the presence of misbehaving nodes. In this work, authors also incorporated a sequential probability ratio test for estimating the mean sample size of attack.

Hernandez-orallo et al. [14] proposed a collaborative watchdog mechanism for detecting selfish nodes in an ad hoc scenario. In this paper, authors incorporated Poisson distribution for analysing cooperativity among the mobile nodes which defines two states for collaborative nodes viz., NOINFO and POSITIVE states. A NOINFO state of collaborative node is the state in which the particular node does not realize its neighbours' selfish behaviour, while in case of POSITIVE state, an individual mobile node acknowledges the

neighbouring selfish nodes. Authors have incorporated continuous time Markov chain (CTMC) for modeling the network, and the network is evaluated collaboratively using watchdog. This model also aids in determining the time and cost incurred in the detection of selfish nodes with the aid of watchdog mechanism.

Xing in [15] further contributed a novel approach based on generic semi-Markov model for characterizing nodes' behaviours and their transitions. This approach also adapts stochastic properties for framing transient and limited probabilities for mobile nodes which aids in estimating the negative impact of nodes' misbehaviour and the node failures. Lei Guang et al. [16] contributed a novel approach known as probabilistic random back off which is capable of mitigating selfish nodes. This mechanism mitigates the selfish nodes which specifically drops others nodes' packets without forwarding it to the next hop neighbour in the routing path. This model incorporates 3-D Markov chain for analysing the characterization behaviour of mobile nodes towards network survivability.

Furthermore, the benchmark systems used for comparing the proposed FTCSPM approach are discussed below.

Komathy and Narayanasamy [17] developed a probabilistic behaviour model (PBM) based on nodes' residual energy for synchronizing collaborative mobile nodes. This approach measures the trade-off that exists between the energy parameters (residual energy and energy utilization) and network parameters (packet delivery ratio and average end-end delay). This probabilistic model also predicts the expected node behaviour which highly depends upon the packet delivery and drop ratio. For this prediction, they incorporated a dynamic memory table called neighbour table which regularly estimates the forwarding rates of neighbour nodes. Finally, the network reliability is manipulated based on the equilibrium value of a mobile node that quantifies the influence of other neighbouring mobile nodes towards them by means of packet delivery rate and end-end delay.

Azni et al. [18] contributed a correlated node behavior model (CNBM) based on continuous time semi-Markov process for clustering the mobile nodes. This model characterizes the node behaviour based on probability of selfishness, probability of forwarding packets, probability of dropped packets and probability of recovery. Further, authors contributed [19] an epidemic correlated node behavioral model (ECNBM) to characterize the behaviour of the mobile nodes participating in the routing path. The ECNBM approach isolates the malicious nodes from the ad hoc environment in two phases, the first phase characterizes the behaviour of the mobile node and its dynamic transition in behaviour states based on semi-Markov process. The second stage derives the predicted correlation degree of a mobile node from its current state behavioural characteristics.

Further, PBM, CNBM and ECNBM are mainly considered for comparison since they are proven as the significant and primary semi-Markov-based correlated node behaviour models for efficient and effective isolation of selfish nodes. In addition, PBM, CNBM and ECNBM detect selfish nodes rapidly and improve the survivability of the network by 33 % than other existing works available in the literature.

2.1 Extract of the literature

The forecasting models available in the literature for mitigating selfish nodes have the following shortcomings.

a) A semi-Markov-based selfish behaviour forecasting model that utilizes non birth-death process has not been explored to the best of our knowledge.
b) A forecasting mechanism that incorporates the futuristic trust coefficient for mitigating selfishness in order to enable high survivability in an ad hoc network has not been investigated.

Hence, these limitations motivated us to devise a futuristic trust coefficient-based semi-Markov prediction model for isolating selfish behaviour of nodes.

3 Futuristic trust coefficient-based semi-Markov prediction model

FTCSPM is a non birth-death process based semi-Markov prediction model proposed for mitigating selfish nodes. It identifies and isolates the selfish nodes from the routing path based on a factor called a futuristic trust coefficient. This coefficient quantifies the likelihood probability for a mobile node to get transited into a selfish node. It also aids in framing a lower and upper bound of connectivity under which the survivability of the entire network is optimal. Further, FTCSPM is a distributed mechanism for detecting and isolating selfish nodes, in which the reputation is calculated in each and every mobile node rather than any centralized node. This distributed mechanism implemented in FTCSPM certainly increases the overhead which is negligibly small and further, it is experimentally tested and detailed in Section 5.

Thus, "*Given a wireless ad hoc network 'N' with possible definitions of mobile node behaviours 'B', the problem can be formulated as a network survivability model 'M* (*N*,*B*)*' that estimates and isolates the selfish nodes from the routing path through futuristic trust coefficient which quantifies the likelihood probability incurred by a mobile node to get transited into the non-cooperative state*".

The FTCSPM approach detects and isolates selfish behaviour of mobile nodes through the following steps.

a) Estimation of stochastic properties from mobile nodes.
b) Estimation of model parameters
c) Node behaviour modeling-based transition probability matrix
d) Manipulation of futuristic trust coefficient-based on non birth-death semi-Markov process.
e) Isolation of selfish nodes based on futuristic trust coefficient.

3.1 Estimation of stochastic properties from mobile nodes

The stochastic properties of a mobile node are estimated through the input parameters that are extracted from the packets forwarded between the source and destination nodes. These input parameters contain information related to a) number of packets forwarded by a mobile node, b) number of packets received by a mobile node and c) residual energy of a mobile node. The derived stochastic properties portray the exhaustive set of all possible behaviours that a mobile node could exhibit during data dissemination. These stochastic properties are derived by means of random process which is defined as a Markov process $M(t)$ such that, the value of $M(f)$, for $f > t$ does not depends upon the value of $M(h)$, for $h < t$. In other words, these Markovian-based stochastic properties depicts that the identification of a node behaviour is forecasted only based upon its present stochastic values and not based on the past observations. Hence, these stochastic properties have limited historical dependence. The sequence of states in this Markov process is said to be a Markov chain $\{M_n\}$ at time t_n, since this process forecast the future behaviour M_{n+1} depending only on the present state M_n and not on the past behaviour $M_{n-1}, M_{n-2}, \ldots, M_0$. In this model, the nodes are categorized into three states viz., cooperative, selfish and failed. This model is even represented as a three state Markov process as represented in Fig. 1, which adequately emphasizes on the mobile nodes' behaviour during routing process.

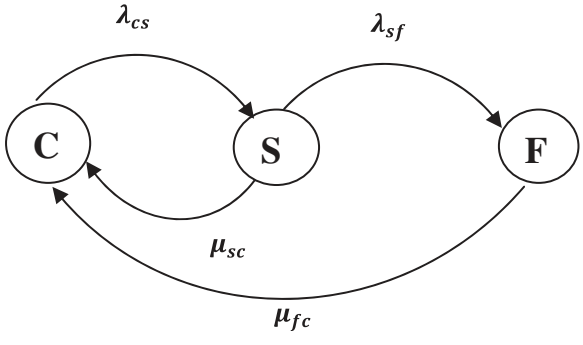

Fig. 1 Transition model representing exhaustive set of node behaviours

3.2 Estimation of stochastic probabilities

The stochastic probabilities derived from the stochastic properties are classified as follows:

- λ_{cs}—stochastic probability for a cooperative mobile node to turn into selfish node
- μ_{sc}—stochastic probability for a selfish node to rehabilitate into cooperative mobile node
- μ_{sf}—stochastic probability for a cooperative mobile node or a selfish node to turn into failure node.
- μ_{fc}—stochastic probability for a failure node to rehabilitate into cooperative mobile node

The stochastic probabilities as defined above are computed in terms of network parameters. AODV uses HELLO message as the periodical broadcasting message to update its connectivity information with their neighbours. In each of the simulation run, the first initiated HELLO control packet is utilized to relay the information regarding residual energy of each and every mobile node. Further, the mean lifetime of the node can be derived from the ratio of residual energy possessed by a mobile node to the amount of remaining energy present in the mobile after transmitting 'N' number of packets as given in (1),

$$L_T = \frac{E_R}{E_R - E_N} \tag{1}$$

where E_R is the residual energy possessed by a mobile node and E_N is the energy required for transmitting maximum of 'N' number of packets.

Furthermore, a cooperative mobile node denies forwarding its neighbour nodes' packets when its residual energy goes below the value of $^1/_\tau$ of its initial energy as defined in [20]. Hence, we can say that a cooperative node becomes selfish at time 't' is given through (2)

$$S(t) = (1-1/\tau)L_T \tag{2}$$

where τ is the selfish threshold parameter and L_T is the mean lifetime of the mobile node.

The probability of packet dropping due to selfishness at a given time instant 't' is by (3) and (4),

$$\lambda_{cs} = 1/S(t) \tag{3}$$

$$\lambda_{cs} = \frac{\tau}{\tau-1} * \frac{1}{L_T} \tag{4}$$

Hence, a mobile node is considered to be highly cooperative when the value 'λ_{cs}' is very less, and it also infers that the particular node has very high mean life time.

Similarly, mobile node may change its state from selfish to cooperative. This transition is identified based on the stochastic probability ''μ_{sc}' computed through the ratio of maximum number of packets forwarded by a mobile node for the sake of their neighbours to the maximum number of packets received by that mobile node from their neighbours as defined in (5).

$$\mu_{sc} = \frac{M_{np(f)}}{M_{rp(r)}} \tag{5}$$

Further, this stochastic probability is computed from the direct trust value identified between the neighbouring nodes of a routing path based on mutual packet forwarding process.

This direct thrust value identified gives a clear picture on the level of cooperation extended by a mobile μsc node to their neighbour. Thus, a mobile node in selfish mode gets into cooperative when the value of μsc reaches above a threshold as defined in [21].

Furthermore, a mobile node either in cooperative or selfish state may either turn into failure state. This transition is confirmed based on stochastic probability λ_{sf}, which is defined through the ratio of maximum number of packets dropped by the mobile node to the maximum number of packets received by the mobile node from its neighbours as given by (6)

$$\lambda_{sf} = \frac{M_{np(d)}}{M_{np(r)}} \tag{6}$$

This stochastic probability λ_{sf} is actually calculated only when the path loss between the mobile nodes of a routing path reaches below a link threshold level as defined in [22] and derived through (7)

$$M_{LIN-LOSS} = \frac{E_N}{Ad^2k} \tag{7}$$

where 'd' and 'k' denote the average distance of communication between mobile nodes and mobility proportion variable, respectively.

Finally, a mobile node in a failure state may get rehabilitated into a cooperative node and can enter into the network through proper reconfiguration. This rehabilitation probability of a mobile 'μ_{fc}' depends upon the mean time required for reconfiguration as defined by (8)

$$\mu_{fc} = \frac{1}{MTRR} \tag{8}$$

Therefore, a mobile node can reconfigure and enter into the network when the mean reconfiguration time of the network is minimum.

3.3 Node behaviour modeling through transition probability matrix

From the model parameters, the probabilities of λ_{cs}, μ_{sc}, $\lambda_{sf/cf}$ and μ_{fc} are derived. Further, the Markov chain representing the possible behaviour for a mobile node at time instant 't' is formally represented through (9)

$$\begin{aligned}
\lambda_{cs} &= P\left[M_{t-1}^{(i)} = C/M_t^i = S\right] \\
\mu_{sc} &= P\left[M_{t-1}^{(i)} = S/M_t^i = C\right] \\
\lambda_{sf} &= P\left[M_{t-1}^{(i)} = S/M_t^i = F\right] \\
&\quad or \\
p\left[M_{-1}^{(i)} = C/M_t^i = F\right] \\
\mu_{fc} &- P\left[M_{t-1}^{(i)} = F/M_t^i = C\right]
\end{aligned} \tag{9}$$

In the above representation, it is assumed that the stochastic probability of a node to convert from selfish to failure is equivalent to the stochastic probability of a cooperative node for turning into failure as defined in [23].

In addition, from the extracted exhaustive set of node behaviours, a Markov-based transition probability matrix can be formulated as below in (10).

$$T_{p(u)} = \begin{bmatrix} 1-(\lambda_{cs}+\lambda_{csf}) & \mu_{cs} & \mu_{sf} \\ \mu_{sc} & 1-(\mu_{sc}+\lambda_{sf}) & \lambda_{sf} \\ \mu_{fc} & 0 & 1-\lambda_{fc} \end{bmatrix} \tag{10}$$

This transition matrix provides a snapshot about the possible behavioural transitions of a mobile node during the routing activity. The entry '0' in the transition matrix emphasizes that this model does not consider the transition of a mobile node from the failed state to a selfish state into account.

3.4 Manipulation of futuristic trust coefficient-based on non birth-death semi-Markov process

In FTCSPM, the stochastic probabilities derived are designated into failure time distributions (λ_{cs}, λ_{sf}) and repair time distributions (μ_{sc}, μ_{fc}). Further, the failure time distributions are assumed to be exponential but the repair time distributions can be divided into two phases viz., i) rehabilitating selfish nodes to cooperative nodes and ii) rehabilitating failure nodes to cooperative nodes.

These two repair phases are exponentially distributed with the expectation coefficient of $1/\mu_{sc}$ and $1/\mu_{fc}$, respectively. Furthermore, in this non birth-death process, the cumulative sojourn period during failure is two staged and hypo-exponential distribution, the FTCSPM approach is a semi-Markov prediction process rather than a homogeneous continuous time Markov chain. In

this model, the steady state probability vectors for detection are considered as (π_c, π_S, π_F).

In this vector, π_c indicates the steady state probability of a mobile node during cooperation, while π_S indicates the steady state probability of a mobile node during selfishness (futuristic trust coefficient) and π_F the steady state probability of a mobile node under failure.

From the state diagram, it is transparent that this mechanism is a non birth-death process. Since there is direct transition from state '*F*' to state '*C*', the balance equations of the FTCSPM approach is represented through (11), (12) and (13).

$$\lambda_{cs}\pi_c = \mu_{fc}\pi_F + \mu_{SC}\pi_S \tag{11}$$

$$\lambda_{cs}\pi_c = \lambda_{sf}\pi_S + \mu_{SC}\pi_S \tag{12}$$

and

$$\mu_{fc}\pi_F = \lambda_{sf}\pi_S \tag{13}$$

From (12), the futuristic trust coefficient of selfishness in terms of cooperative probability is derived through the steps (14) and (15),

$$\lambda_{sf}\pi_S = (\lambda_{cs}\mu_{sc})\ \pi_c \tag{14}$$

$$\pi_S = \frac{(\lambda_{cs} - \mu_{sc})}{\lambda_{sf}}\pi_c \tag{15}$$

Similarly from (13), the steady state probability of a mobile node under failure is computed through steps (16) and (17),

$$\pi_F = \frac{\lambda_{sf}}{\mu_{fc}}\pi_S \tag{16}$$

$$\pi_F = \frac{\lambda_{sf}}{\mu_{fc}}\ \frac{(\lambda_{cs} - \mu_{sc})}{\lambda_{sf}}\ \pi_C \tag{17}$$

Then, the steady state probability vector [π_c, π_S, π_F] of a mobile node in terms of stochastic probabilities are represented through (18), (19) and (20)

$$\pi_C = \frac{\lambda_{sf\ \mu fc}}{(\lambda_{sf} - \mu_{SC})\mu_{fc} + (\mu_{fc} + \lambda_{sf})\lambda_{SC} - \mu_{CS-}\mu_{SC}\lambda_{CS}} \tag{18}$$

$$\pi_S = \frac{(\lambda_{cs-}\mu_{sc})\mu_{fc}}{(\lambda_{sf-}\mu_{sc})\mu_{fc} + (\mu_{fc} + \lambda_{sf})\lambda_{cs} - \mu_{sc}\mu_{fc}} \tag{19}$$

$$\pi_F = \frac{(\lambda_{sf-}\lambda_{cs})\mu_{sc}}{(\lambda_{cs-}\mu_{sc})\mu_{sf} + (\mu_{fc} + \lambda_{sf})\lambda_{cs} - \mu_{sc}\mu_{fc}} \tag{20}$$

Since

$$\pi_C + \pi_S + \pi_F = 1 \tag{21}$$

From the derived vector, the Futuristic trust coefficient π_S aids in quantifying the degree of selfish behaviour attributed by a mobile node.

3.5 Isolation of selfish nodes based on futuristic trust coefficient

In this model, the mobile nodes are identified as selfish when the value of π_S reaches below the futuristic trust threshold of 0.6 as defined in [24]. Then, the FTCSPM approach isolates the selfish nodes based on the value of futuristic trust coefficient π_S possessed by each of the mobile node for enabling reliable routing path.

4 Validation and network survivability analysis of FTCSPM Model

The proposed FTCSPM approach is validated by utilizing the data that are collected through simulation and Weibull distribution for comparative analysis. Weibull distribution is mainly incorporated, since it is considered as the significant distribution used for modeling the lifetime events in case of reliability engineering. In this validation, the time required for a mobile node to get transited into a selfish node ($F_S(t)$) is manipulated through Weibull distribution by using (21) as defined in [19]

$$F_s(t) = 1 - e^{-\left(t/\beta\right)^a} \tag{22}$$

Moreover, the mean transition time incurred in the conversion of a cooperative mobile node into a selfish node is identified as 6.49 s. Hence, we choose $a = 2$ and $\beta^S = 6$ from simulation.

From Fig. 2, it is transparent that the results obtained through Weibull distribution have high degree of correlation with the simulation results. It is also clear that the maximum and minimum time incurred for identifying the selfish behaviour on a mobile node is between 140 and 180 s.

In this approach, survivability of networks in the presence of selfish mobile nodes is quantified through selfish survivability factor which is defined as the ratio of observed number of mobile nodes infected through selfishness to the expected number of mobile nodes actually infected. Further, the selfish survivability factor infers that FTCSPM in an average withstands the degree of selfishness up to a maximum of about 39 % when compared to CNBM, PBM and ECNBM.

5 Simulation results and analysis

In this section, the performance analysis of the proposed FTCSPM is evaluated through simulation using ns2 (v.2.32). In this simulation experiments, the network area is 1000 × 1000 m^2 approximately. The number of nodes considered in the network area is ranging from 50 to 100 in order to represent small and large networks. Further, in this simulation, random waypoint model is considered as mobility model since it generates more realistic node movement patterns. The traffic pattern of the simulated network model is represented in terms of

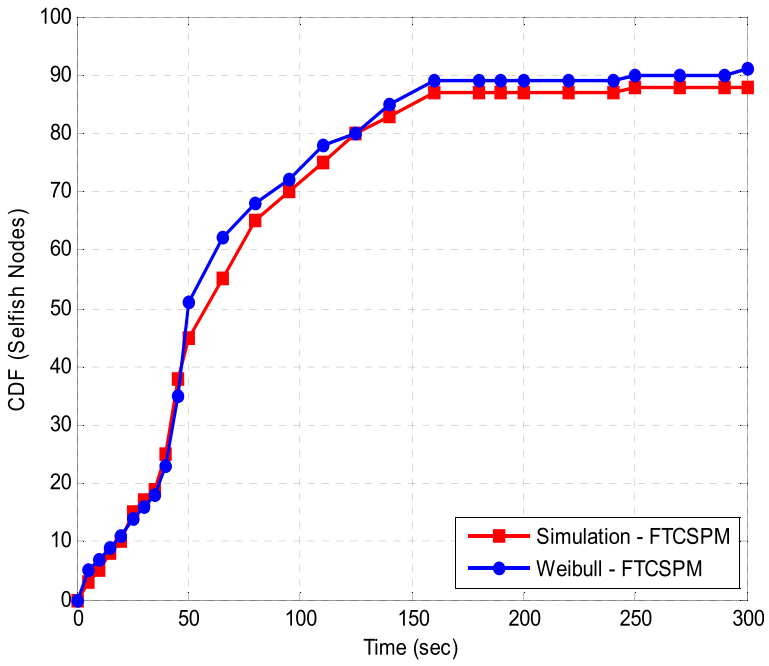

Fig. 2 Validation graph of FTCSPM based on Weibull distribution and simulations

constant bit rate (CBR) of 40 packets per second. The simulation time is set to 250 s, so that the results are derived in various simulation rounds before the system reaches its steady state. Table 1 depicts the simulation parameters setup for the analysing network performance by incorporating FTCSPM approach.

Further, the main objective of these simulation experiments is to evaluate the correctness of the proposed FTCSPM approach. Hence, the efficiency of the proposed FTCSPM is proved not only through comparative analysis with the existing algorithms viz., CNBM, PBM and ECNBM, but also by incorporating a similar network configuration for implementing FTCSPM and the three benchmark mitigation mechanisms.

Table 1 Simulation configuration

Parameter	Value
NS version	2.32
Number of nodes	100
Protocol used	AODV
Mac layer	802.11
Terrain area	1000 × 1000 m^2
Mobility model	Random way point
Simulation time	250 s
Traffic model	CBR (40 packets/s)
Packet size	512 bytes
Type of antenna	Antenna/omni antenna
Type of propagation	Two-way ground
Channel capacity	2 Mpbs

Furthermore, in simulation experiments, the change in behaviours of a mobile node according to the strategies defined in Section 3 is analysed. The routing protocol is chosen here is AODV, which is implemented to route the data packets using cooperative nodes of the network environment, while for routing data packets to the destination in the presence of selfish nodes is carried out through modified version of AODV so that the selfish mobile nodes are isolated without affecting the standard network activities.

In addition, the connectivity of an ad hoc network purely depends on the cooperation established by the intermediate nodes towards the establishment of a reliable routing path [25–29]. However, the connectivity is drastically influenced by the presence of selfish nodes, since these node decreases the packet delivery ratio and throughput while increasing the energy consumption rate, packet drop rate and average end-to-end delay [30, 31]. Hence, the performance of the proposed FTCSPM is evaluated based on performance evaluation parameters viz., packet delivery ratio, energy consumption, average end-to-end delay, packet drop rate and throughput.

Packet delivery ratio (PDR):

It is defined as the ratio between the number of packets received by the destination node and the number of packets sent to the destination node.

Energy consumption rate:

It is defined as the total energy consumed by a mobile node during the state of transmission, reception, idle and sleep.

Average end-to-end delay:

It is defined as the average time taken by the data packets to reach its destination including the time taken for connection establishment and queuing delay.

Packet drop rate:

It is defined as the total number of data packets lost during the data transmission from source to the destination.

Throughput:

It is defined as the total number of packets successfully delivered to the destination in a specified period.

5.1 Performance evaluation of FTCSPM by varying the number of mobile nodes (experiment 1)

The main aim of this experiment is to evaluate the performance of the proposed FTCSPM approach by varying the number of mobile nodes present in the environment. In this experimental analysis, the number of mobile nodes is varied from 20 to 100 in increments of 20 in which 7 % of the mobile nodes is considered as selfish. Figure 3a–e depicts the plots of packet delivery ratio, energy consumption rate, average end-to-end delay, packet drop rate and throughput for various selfish mitigation mechanisms such as FTCSPM, CNBM, PBM and ECNBM.

In general, the packet delivery ratio of a network decreases when there is an increase in the number of transmitting mobile nodes. This decrease in PDR value is mainly due to inadequate availability of bandwidth caused by enormous data generation. The plots depicted in Fig. 3a shows the packet delivery ratio exhibited by FTCSPM and the three benchmark mitigation mechanisms. However, the proposed mechanism FTCSPM shows considerable improvement in packet delivery rate when compared to the other three benchmark mechanisms. FTCSPM also exhibits an increase in PDR from 8 to 14 % than ECNBM, from 16 to 22 % than CNBM and from 19 to 25 % than PBM. On the whole, the proposed FTCSPM shows a significant improvement in packet delivery ratio by 14.2 %.

Similarly, the plots depicted in Fig. 3b shows the energy consumption rate of FTCSPM with the three benchmark systems. The energy consumption rate considerably increases when the number of mobile nodes participating in the transmission increases due to enormous amount of data flow. But the proposed FTCSPM shows significant improvement in performance by consuming the minimum energy even when enormous amount of data is transmitted. This is due to the effectiveness of the FTCSPM approach in predicting the change in behaviour of the mobile nodes during the period of transmission. FTCSPM also shows a decrease of 0.7 to 1.1 J of energy consumption from ECNBM, from 0.9 to 1.2 J from CNBM and from 1.8 to 2.2 J from PBM. In an average, FTCSPM shows considerable decrease in energy consumption rate of 2.34 J when compared to the other three selfish mitigation mechanisms.

Further, Fig. 3c depicts the plots of average end-to-end delay for the given number of mobile nodes of the four mitigation mechanisms viz., FTCSPM, CNBM, PBM and ECNBM. The proposed method FTCSPM shows a significant decrease in average end-to-end delay, since FTCSPM incorporates an effective and efficient selfishness isolation approach for enabling reliable routing path for data transmission. FTCSPM shows a decrease of 9 to 12 % in average end-to-end delay from ECNBM, from 14 to 19 % from CNBM and from 16 to 22 % from PBM. FTCSPM also decreases the average end-to-end delay factor by 37 % (mean value), when compared to the other three benchmark mechanisms.

Furthermore, Fig. 3d depicts the plots of packet drop rate derived for a given number of mobile nodes from all the four selfish mitigation mechanisms. The packet drop rate increases when the number of mobile nodes increases since large number of data packets has been transmitted. However, the proposed FTCSPM approach considerably decreases the packet drop rate due its in-built trust-based prediction mechanism for analysing change in behaviour of mobile nodes. Further, FTCSPM shows a decrease of 10 to 15 % in packet drop rate than ECNBM, from 15 to 22 % than CNBM and from 21 to 29 % than PBM. FTCSPM in an average decreases the packet drop rate by 28 % than the other three mitigation mechanisms.

Finally, Fig. 3e depicts the plots of throughput derived for a given number of mobile nodes from all four selfish mitigation mechanisms. The throughput decreases when the number of selfish nodes increases since increase in packet drop rate reduces the throughput. However, the proposed FTCSPM approach considerably increases the throughput of the network when compared to ECNBM, CNBM and PBM. Further, FTCSPM shows increase of 9 to 14 % in throughput from ECNBM, from 12 to 16 % than CNBM and from 14 to 19 % than PBM. Furthermore, FTCSPM increases the throughput in an average value by 23 % than the other three selfish mitigation mechanisms used for benchmarking.

5.2 Performance evaluation of FTCSPM by varying the number of selfish nodes (experiment 2)

The main objective of this experiment is to prove the superior performance of the proposed FTCSPM approach with the other three benchmark systems by varying the number of selfish nodes present in the network. In this experimental analysis, the number of selfish nodes is

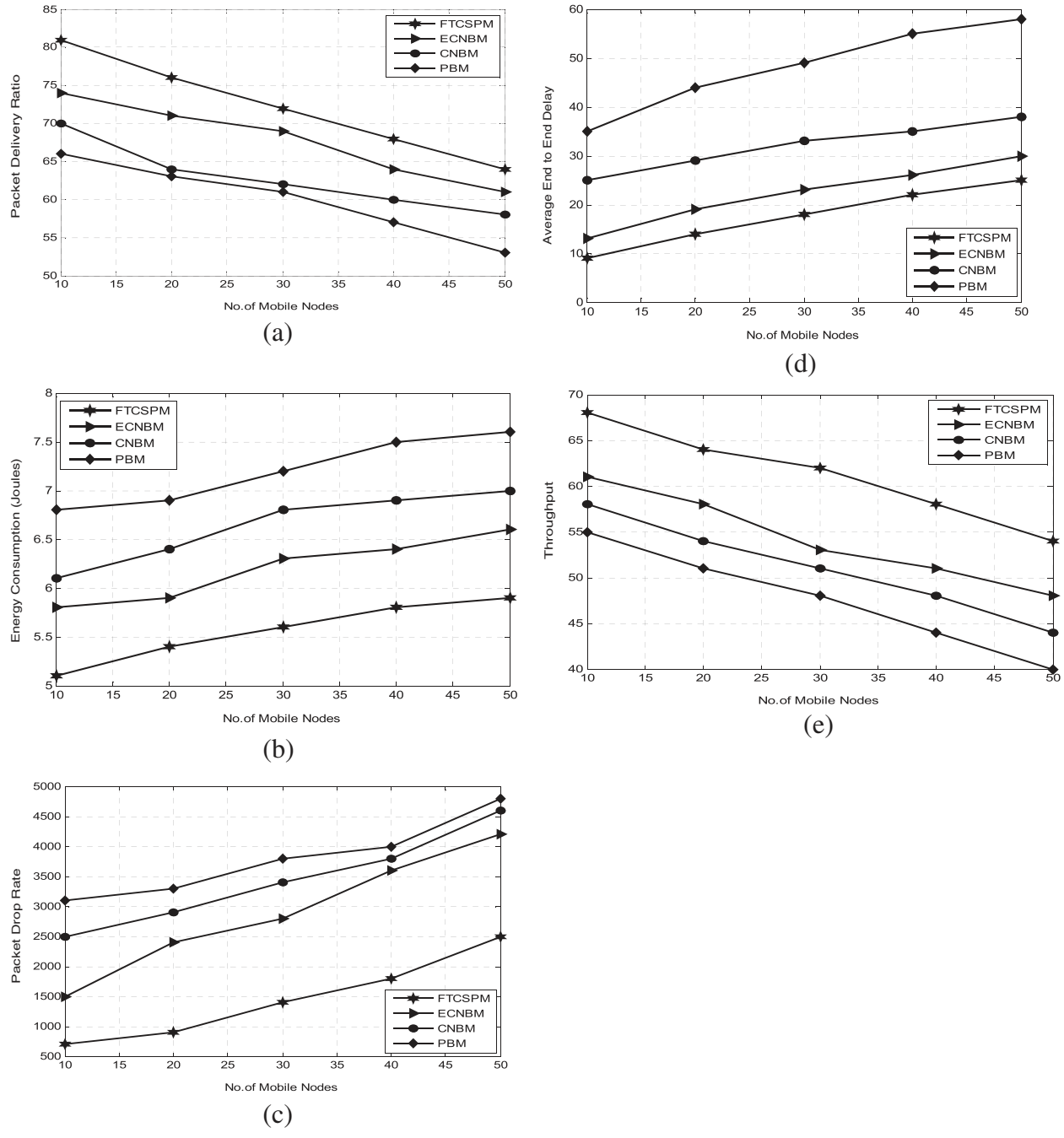

Fig. 3 Comparison of FTCSPM with CNBM, PBM and ECNBM based on (**a**) packet delivery ratio, (**b**) energy consumption rate, (**c**) average end-to-end delay, (**d**) packet drop rate and (**e**) throughput by varying the number of mobile nodes

varied from 5 to 25 in the increments of 5. Figure 4a–e depicts the plots of packet delivery ratio, energy consumption rate, average end-to-end delay, packet drop rate and throughput derived for comparing the selfish mitigation mechanisms like FTCSPM, CNBM, PBM and ECNBM.

The plots depicted in the Fig. 4a shows that there is decrease in packet delivery ratio exhibited by all of the above said four mitigation mechanisms when the number of selfish nodes increases in the ad hoc environment. However, the proposed mechanism FTCSPM shows a considerable improvement in packet delivery rate when compared to the other three benchmark mechanisms. FTCSPM also shows an increase in PDR from 9 to 14 % than ECNBM, from 12 to 16 % than CNBM and from 17 to 21 % than PBM. On the whole, FTCSPM shows a

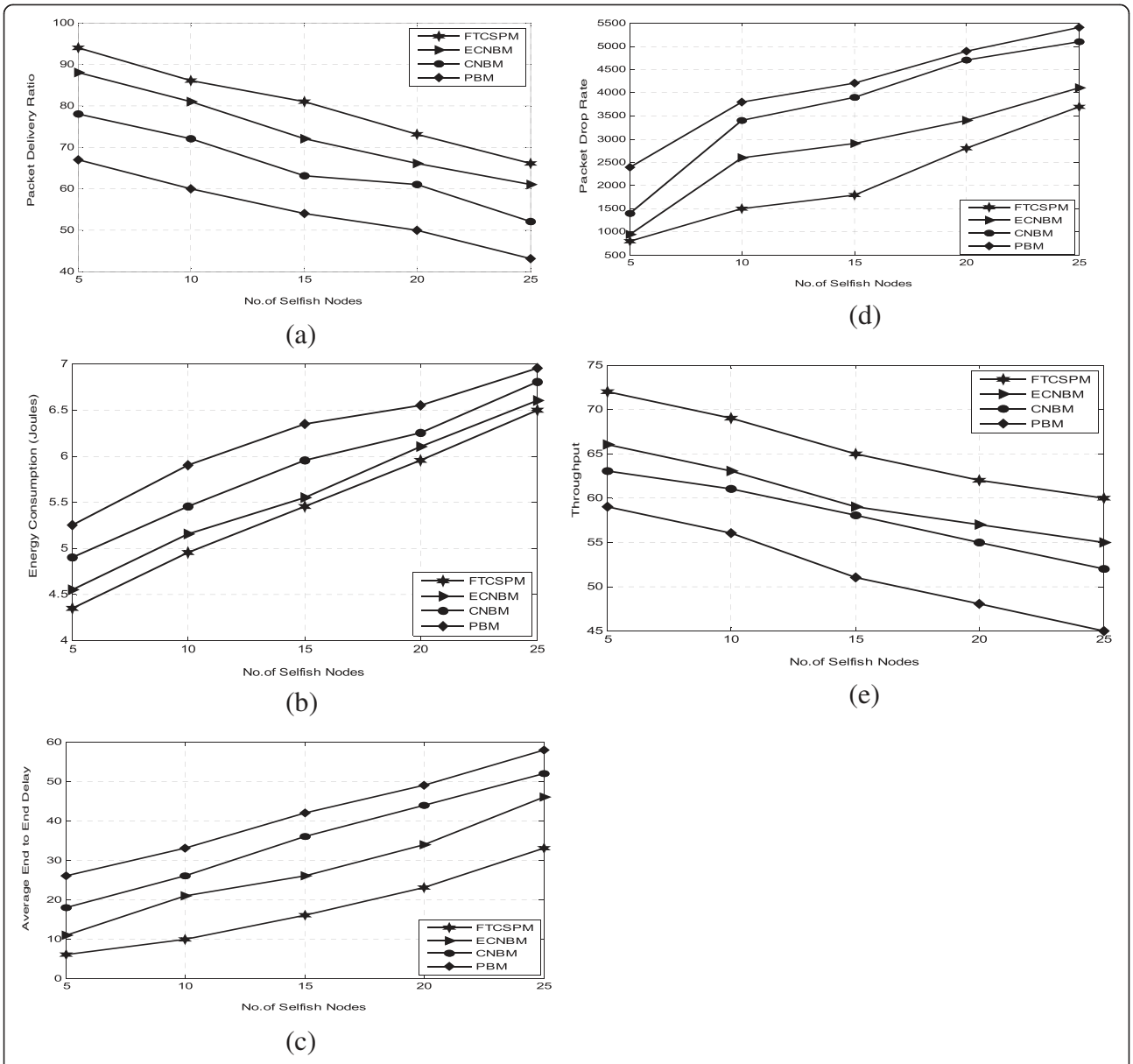

Fig. 4 Comparison of FTCSPM with CNBM, PBM and ECNBM based on (**a**) packet delivery ratio, (**b**) energy consumption rate, (**c**) average end-to-end delay, (**d**) packet drop rate and (**e**) throughput by varying the number of selfish nodes

significant improvement in packet delivery ratio by 24.4 %.

Similarly, the plots depicted in Fig. 4b shows energy consumption rate for the given number of mobile nodes in order to deliver the data packets reliably. The energy conservation factor considerably increases when the number of selfish mobile nodes increases in the ad hoc environment. But the proposed FTCSPM shows significant improvement in performance by conserving minimum energy. Further, FTCSPM shows decrease of 1.4 to 1.9 J of energy consumption from ECNBM, from 1.9 to 2.7 J from CNBM and from 2.4 to 3.8 J from PBM. In an average, FTCSPM shows considerable decrease in energy consumption rate of 5.67 J when compared to the other three selfish mitigation mechanisms.

Figure 4c depicts the plots of average end-to-end delay for the given number of selfish nodes from the four mitigation mechanisms viz., FTCSPM, CNBM, PBM and ECNBM. The proposed FTCSPM shows the decrease of 8 to 15 % in average end-to-end delay from ECNBM, from 18 to 22 % from CNBM and from 23 to 28 % from PBM. Furthermore, FTCSPM decreases the average end-to-end delay factor by 25.54 % (mean value), when compared to all the other three mitigation mechanisms.

Figure 4d depicts the plots of packets drop rate considered for comparative analysis for the four selfish

mitigation mechanisms. The packet drop rate increases when the number of selfish nodes increases since it does not forward or cooperate with the other mobile nodes present in the routing path. However, the proposed FTCSPM approach considerably decreases the packet drop rate from 10–17 % than ECNBM, from 15–25 % than CNBM and from 21–27 % than PBM. FTCSPM also decreases the packet drop rate in an average by 24.45 % than the other three mitigation mechanisms.

In addition, Fig. 4e depicts the plots for thought derived from all the four selfish mitigation mechanisms. The throughput decreases when the number of selfish nodes increases. However, the proposed FTCSPM approach considerably increases the throughput of the network when compared to ECNBM, CNBM and PBM. Further, FTCSPM shows increase of 11–14 % in packet drop rate from ECNBM, from 14–19 % than CNBM and from 16 to 20 % than PBM. FTCSPM in an average increases the throughput by 19.18 % than the other three selfish mitigation mechanisms.

5.3 Performance evaluation of FTCSPM by varying the CBR traffic flows (experiment 3)

The main goal of this experiment is to prove the superiority of the proposed FTCSPM approach with the other three benchmark systems by varying the CBR traffic flows of the network. In this experiment, the FTCSPM is analysed based on varying CBR traffic flows viz., low (2–4), medium (6), high (8–10). Figure 5a–e presents the comparative analysis plots of packet delivery ratio, energy consumption rate, average end-to-end delay, packet drop rate and throughput derived for comparing the selfish mitigation mechanisms like FTCSPM, CNBM, PBM and ECNBM.

Figure 5a shows that there is a decrease in packet delivery ratio when the CBR traffic flow is varied from low level to high level since heavy packet loss occurs due to network congestion. However, the proposed mechanism FTCSPM shows a considerable improvement in packet delivery ratio than the other three benchmark mechanisms. FTCSPM also shows an improvement in PDR from 16 to 22 % than ECNBM, from 21 to 26 % than CNBM and from 24 to 31 % than PBM. On the whole, FTCSPM shows a considerable improvement in packet delivery ratio by 21.3 %.

Similarly, Fig. 5b shows energy consumption rate for the varying traffic flows. The energy consumption rate considerably increases when the CBR traffic flow rate linearly increases. But the proposed FTCSPM shows significant improvement in performance by consuming minimum energy even during the event of high traffic flows. FTCSPM also shows a decrease of 2.1 to 2.5 J of energy consumption than ECNBM, from 2.3 to 2.8 J than CNBM and from 2.9 to 3.3 J than PBM. In an average, FTCSPM considerably decreases the energy consumption rate by 3.45 J when compared to the other three selfish mitigation mechanisms.

Figure 5c depicts the plots of average end-to-end delay for FTCSPM and the considered benchmark systems obtained by varying the CBR traffic flows. FTCSPM decreases the average end-to-end delay of 11 to 14 % than ECNBM, from 15 to 21 % than CNBM and from 17 to 25 % than PBM. Furthermore, FTCSPM decreases the average end-to-end delay factor by 21.54 % (mean value), when compared to all the other three mitigation mechanisms.

Figure 5d depicts the plots of packet drop rate obtained for comparative analysis of the four selfish mitigation mechanisms derived by varying the number of CBR traffic flows. The packet drop rate increases when the CBR traffic flow increases from lower intensity to higher intensity. However, the proposed FTCSPM approach considerably decreases the packet drop rate from 14 to 19 % than ECNBM, from 18 to 22 % than CNBM and from 23 to 29 % than PBM. FTCSPM also decreases the packet drop rate in an average by 20.15 % than the other three benchmark mitigation mechanisms.

In addition, Fig. 5e depicts the comparative analysis chart for throughput derived from all the four selfish mitigation mechanisms. The throughput decreases when the number of selfish nodes increases even when the CBR traffic flow increases. However, FTCSPM approach considerably increases the throughput of the network when compared to ECNBM, CNBM and PBM. Further, FTCSPM shows an improvement of 14 to 17 % in throughput than ECNBM, from 18 to 23 % than CNBM and from 23 to 28 % than PBM. FTCSPM in an average increases the throughput by 22.81 % than the other three selfish mitigation mechanisms.

Finally, FTCSPM is also valuated by varying the number of mobile nodes, number of selfish nodes and traffic flow rate based on control overhead and total overhead. FTCSPM in an average decreases the control overhead by 23, 29 and 32 % than the compared ECNBM, CNBM and PBM approaches, respectively. Similarly, FTCSPM in an average decreases the total overhead by 19, 25 and 29 % than ECNBM, CNBM and PBM approaches, respectively.

6 Conclusions

This paper has presented a futuristic trust coefficient-based semi-Markov prediction model formulated through non birth-death process for mitigating selfish mobile nodes in an ad hoc network. The performance of FTCSPM is analysed based on packet delivery ratio, average end-to-end delay, energy consumption rate, packet drop rate and throughput. The experimental

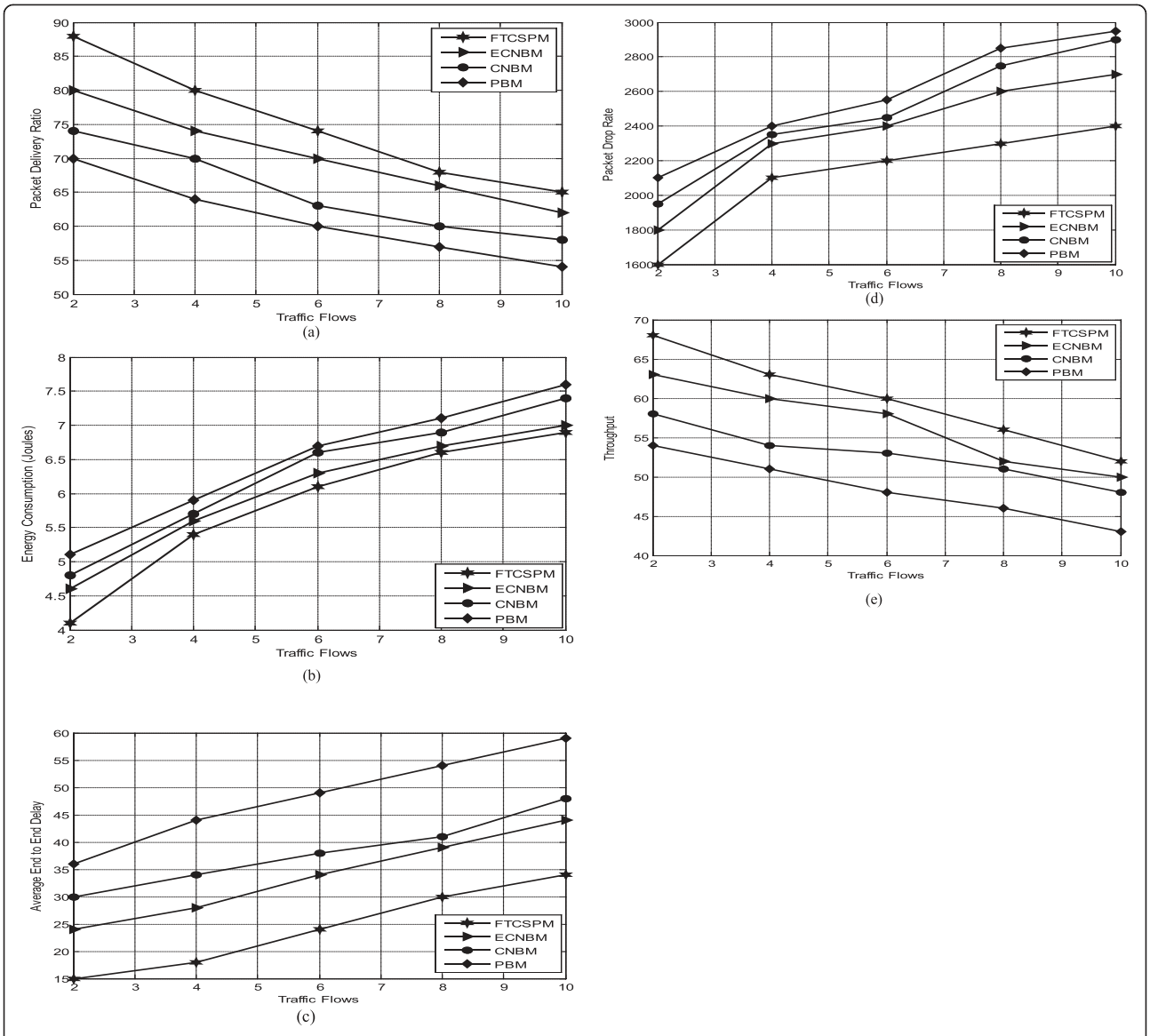

Fig. 5 Comparison of FTCSPM with CNBM, PBM and ECNBM based on (**a**) packet delivery ratio, (**b**) energy consumption rate, (**c**) average end-to-end delay, (**d**) packet drop rate and (**e**) throughput by varying the traffic flow rate

results illustrated in this paper show the proximity performance of the FTCSPM approach with increase in packet delivery ratio and throughput. Further, our ns-2-based simulation study makes it evident that FTCSPM in an average improves the packet delivery ratio and throughput by 14.2 and 23 %, respectively, and at the same time, FTCSPM reduces the energy consumption rate, packet drop rate and average end-to-end delay by 18.4, 37 and 28 %, when compared to the benchmark systems like CNBM, PBM and ECNBM. Further, the influence of selfish nodes towards the survivability of a network is also derived. Furthermore, the proposed model is also validated by means of Weibull distribution, and this validation clearly portrays that Weibull distribution has a high degree of correlation with the simulation results. In addition, FTCSPM detects and isolates the selfish nodes rapidly at the rate of 33 % than the considered benchmark systems.

Finally, as a part of our future work, we have been planning to devise a semi-Markov prediction model based on pure birth-death process that relies only on neighbour-only transitions and a limited availability factor-based semi-Markov prediction model that quantises the degree of participation rendered by the mobile nodes in the routing process.

Competing interests

Both authors declare that they have no competing interests.

Received: 2 March 2015 Accepted: 13 May 2015
Published online: 07 June 2015

References

1. F Xing, W Wang, On the survivability of wireless ad hoc networks with node misbehaviors and failures. IEEE Transactions On Dependable And Secure Computing **7**(3), 284–299 (2010)
2. A Md, AK Akhtar, G Sahoo, Mathematical model for the detection of selfish nodes in MANETs. International Journal of Computer science and Informatics **1**(3), 25–28 (2008)
3. S Buchegger, J-Y Boudec, *Nodes bearing Grudges: Towards routing security, Fairness and Robustness in Mobile Ad-Hoc Network (presented at tenth Euromicro workshop on Parallel, Distributed and Network based Processing* (Canary Islands, Spain, 2002)
4. S Marti, TJ Giuli, K Lai, M Baker, Mitigating routing misbehavior in mobile ad hoc networks. Mobile Computing and Networking **1**(1), 255–265 (2000)
5. SK Hwang, DS Kim et al., Markov model of link connectivity in mobile ad hoc networks. Telecommunication Systems **34**(1–2), 51–58 (2006)
6. L Guang, M Chadi, A Benslimane, Enhancing IEEE 802.11 random backoff in selfish environments. IEEE Transactions On Vehicular Technology **57**(3), 125–132 (2008)
7. G Corradi, J Janssen, R Manca, Numerical treatment of homogenous semi-Markov processes in transient case—a straightforward approach. Methodology and Computing in Applied Probability **6**(1), 233–246 (2004)
8. T Sundarajan, A Shanmugam, Modeling the behavior of selfish forwarding nodes to simulate cooperation in MANET. International Journal of Network Security and Its Application **2**(2), 147–160 (2010)
9. J Sengathir, R Manoharan, A reliability factor based mathematical model for isolating selfishness in MANETs'. International Journal of Information and Communication Technology **6**(3/4), 403–421 (2014)
10. J Sengathir, R Manoharan, Selfish conscious mathematical model based on reliable conditional survivability coefficient in MANET routing, in *3rd Third International Conference on Advances in Information Technology and Mobile Communication (AIM 2013)*. Bangalore, India, April, Proceeding published by Elsevier **1**(1), 31–40 (2013)
11. F Xing, W Wang, *Modeling and analysis of connectivity in mobile ad hoc networks with misbehaving nodes* (Paper presented at the IEEE international conference on communications, IEEE, Istanbul, June, 2006)
12. A Alvaro, Cardenas, R Svetlana, S John Baras, Evaluation of detection algorithms for MAC layer misbehavior. Theory and Experiments. IEEE Transactions on Networking **17**(2), 605–617 (2009)
13. Rohith Dwarakanath Vallam, Antony Franklin A, Siva RamMurthy C, Modelling co-operative MAC layer misbehaviour in IEEE 802.11 ad hoc networks with heterogeneous loads. Paper presented at the 6th international symposium on modeling and optimization in mobile, ad hoc, and wireless networks and workshops, IEEE, WIOPT Berlin, Germany, 1–3 April 2008.
14. E Hernandez-Orallo, MD Serraty, J-C Cano, T Calafate, P Manzoni, Improving selfish node detection in MANETs using a collaborative watchdog. IEEE Letters **16**(5), 642–645 (2012)
15. X Fie, *Modeling, Design, and Analysis on the Resilience of Large-scale Wireless Multi-Hop Networks* (North Carolina State University, Raleigh (North Carolina, USA, Department Of Engineering, 2009)
16. L Guang, M Chadi, A Benslimane, Enhancing IEEE 802.11 random backoff in selfish environments. IEEE Transactions on Vehicular Technology **57**(3), 1806–1822 (2008)
17. K Komathy, P Narayanasamy, A probabilistic behavioral model for selfish neighbors in a wireless ad hoc network. International Journal of Computer Science and Network Security **7**(7), 77–82 (2007)
18. AH Azni, A Rabiah, N Zul, M Azri, B Abd SamadHasan, H Burairah, Correlated node behavior model based on semi Markov process for MANETS. International Journal of Computer Science **9**(1), 25–32 (2013)
19. AH Azni, A Rabiah, N Zul, M Azri, B Abd SamadHasan, H Burairah, Epidermic modelling for correlated node behavior in ad hoc networks. International Journal of Chaotic Computing **1**(1), 22–30 (2013)
20. AP Patil, KDK Rajani, S Bathey, MP Dinesh Kumar, J Malavika, Design of energy efficient routing protocol for MANETs based on AODV. IJCSI **8**(1), 215–220 (2013)
21. Srinivasan V, Nuggehali, Chiasserini, C.F., Rao, R.R., (2003). Stimulating Cooperation in Wireless ad hoc networks. Presented at 22nd Annual Joint Conference of the IEEE Computer and Communication Societies (INFOCOM'03), 2003
22. N Sadagopan, F Bai, B Krihnamachari, A Helmy, PATHS: analysis of PATH duration statistics and their impact on reactive MANET routing protocols. In prod. ACM MobiHoc **1**(1), 299–307 (2003)
23. K Paul, RR Choudhuri, Bandyopadhyay, Survivability analysis of ad hoc wireless network architecture. In prod IFIP-TC6/ European Commission, International Workshop Mobile and Wireless Communication Networks **1**(1), 31–46 (2000)
24. P Manohar, M Vereshechaka, D Manjanth, Survivability, analysis under non-uniform stochastically dependent node damages. National Conference on Communications **1**(1), 1–5 (2010)
25. Y Xu, W Wang, Characterizing the spread of correlated failures in larger wireless networks. In proc. IEEE INFOCOM **56**(11), 1–9 (2010)
26. Z Zhang et al., ECG-cryptography and authentication in body area networks. IEEE Transactions on Information Technology in Biomedicine **16**(6), 1070–1078 (2012)
27. Z Shen et al., Peer-to-peer media streaming: insights and new developments. Proceedings of the IEEE **99**(12), 2089–2109 (2011)
28. A Attar et al., A survey of security challenges in cognitive radio networks: solutions and future research directions. Proceedings of the IEEE **100**(12), 3172–3186 (2012)
29. Z Wan et al., Adaptive unequal protection for wireless video transmission over IEEE 802.11e networks. Multimedia Tools and Applications **1**(1), 345–352 (2013)
30. D He et al., Retrust: attack-resistant and lightweight trust management for medical sensor networks. IEEE Transactions on Information Technology in Biomedicine **16**(4), 623–632 (2012)
31. J Zhou et al., Securing m-healthcare social networks: challenges, countermeasures and future directions. IEEE Wireless Communications **20**(4), 123–134 (2013)